Relazione S5L2 Luca Calvigioni

SCANSIONI NMAP

Traccia: Tecniche di scansione con Nmap Si richiede allo studente di effettuare le seguenti scansioni sul target Metasploitable:

- **OS fingerprint**
- **Syn Scan**
- **TCP connect**
- **Version detection**

E sul target Windows:

- **OS fingerprint**

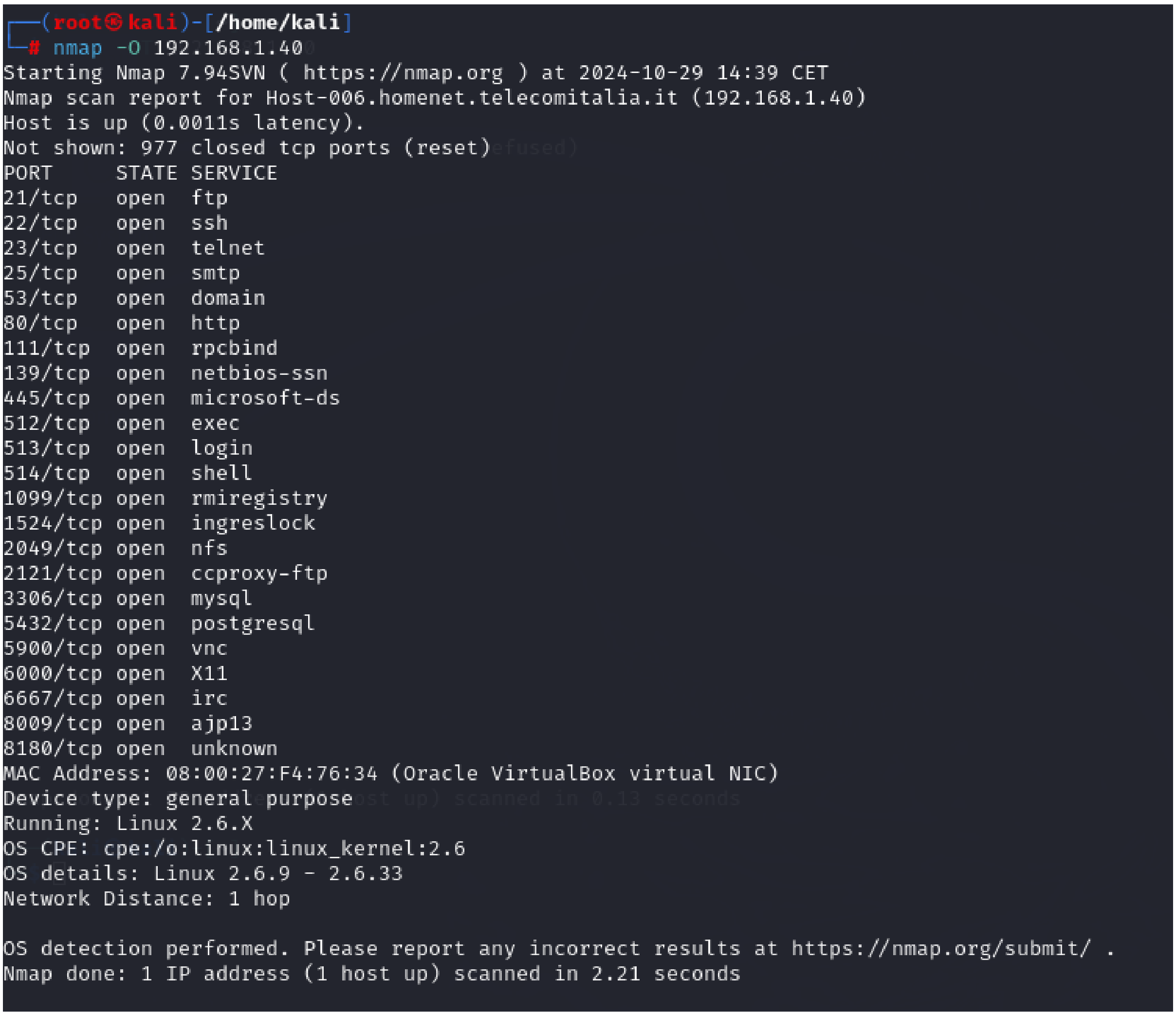
Metasploitable indirizzo ip: 192.168.1.40

OS fingerprint di Metasploitable:

Digitiamo sul terminale di Kali Linux il comando

“nmap –O 192.168.1.40”

una volta terminata la scansione il risultato ci elencherà le porte aperte e i servizi che vengono utilizzati, successivamente il sistema operativo utilizzato.



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.1.40
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 14:39 CET
Nmap scan report for Host-006.homenet.telecomitalia.it (192.168.1.40)
Host is up (0.0011s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:F4:76:34 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.21 seconds
```

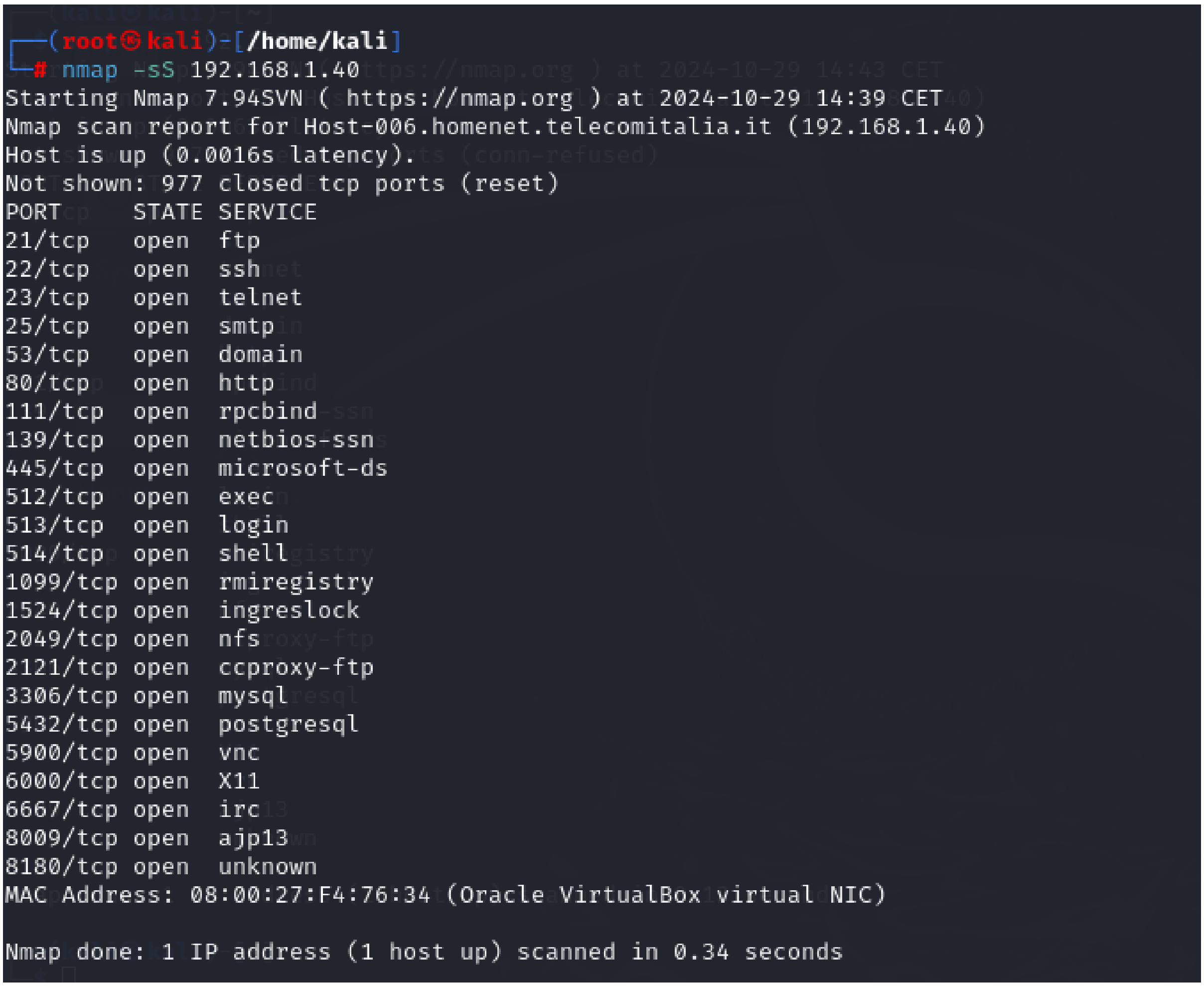
SYN scan di Metasploitable:

Digitiamo sul terminale di Kali Linux il comando

“nmap -sS 192.168.1.40”

Con il comando –sS esegue una “TCP SYN scan” per vedere le porte dei servizi aperte, invia pacchetti SYN senza completare però la stretta di mano a 3 vie

Questa è più furtiva perchè non stabilisce una connessione completa ed è generalmente piu veloce, per eseguirla abbiamo però bisogno dei diritti di Root



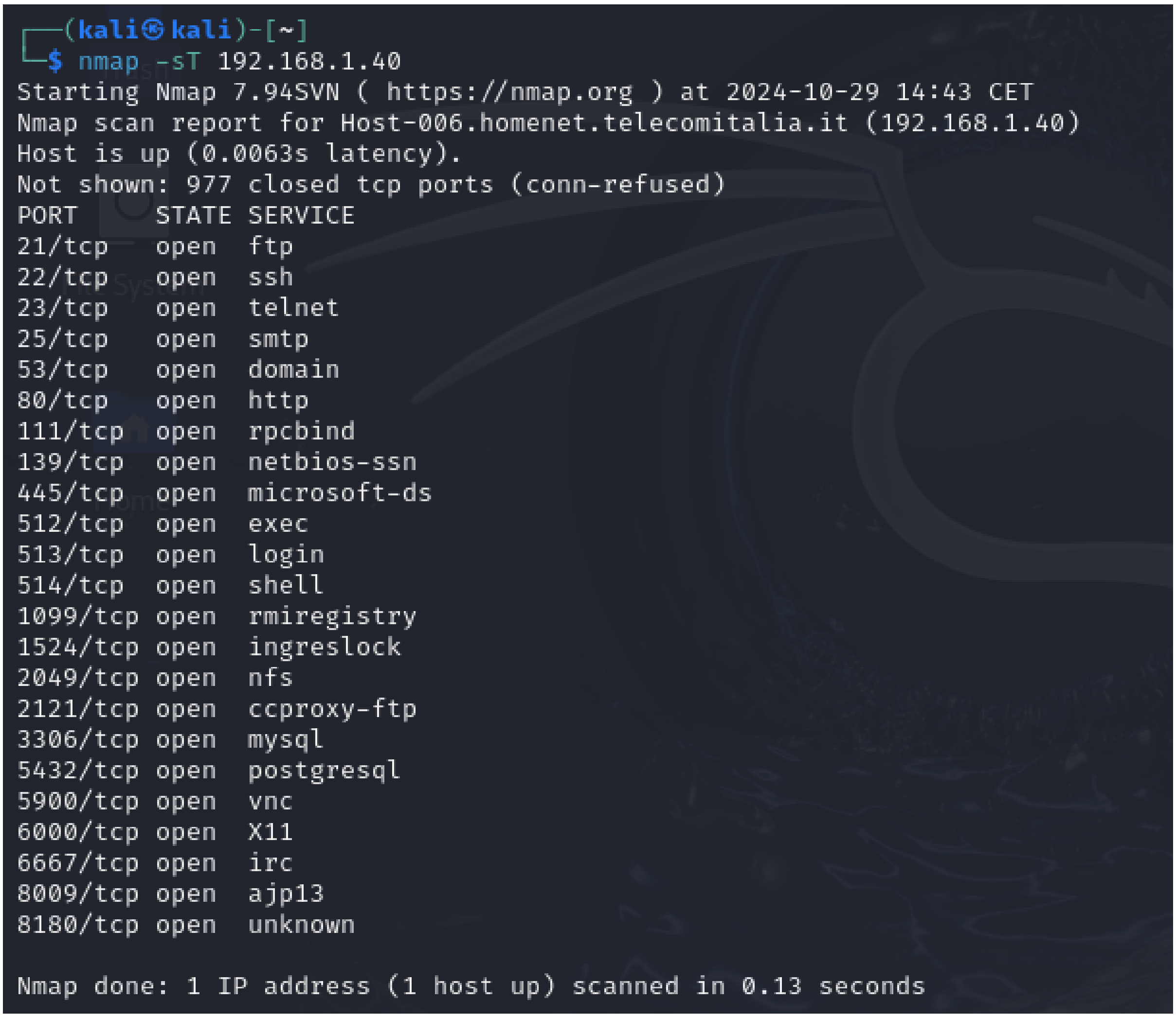
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 192.168.1.40
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 14:39 CET
Nmap scan report for Host-006.homenet.telecomitalia.it (192.168.1.40)
Host is up (0.0016s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:F4:76:34 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
```

TCP connect di Metasploitable:

Digitiamo sul terminale di Kali Linux il comando

“nmap -sT 192.168.1.40”

A differenza di SYN scan, TCP connect fornisce dati più accurati stabilendo connessioni complete (SYN, SYN/ACK, ACK) non servono diritti di Root.



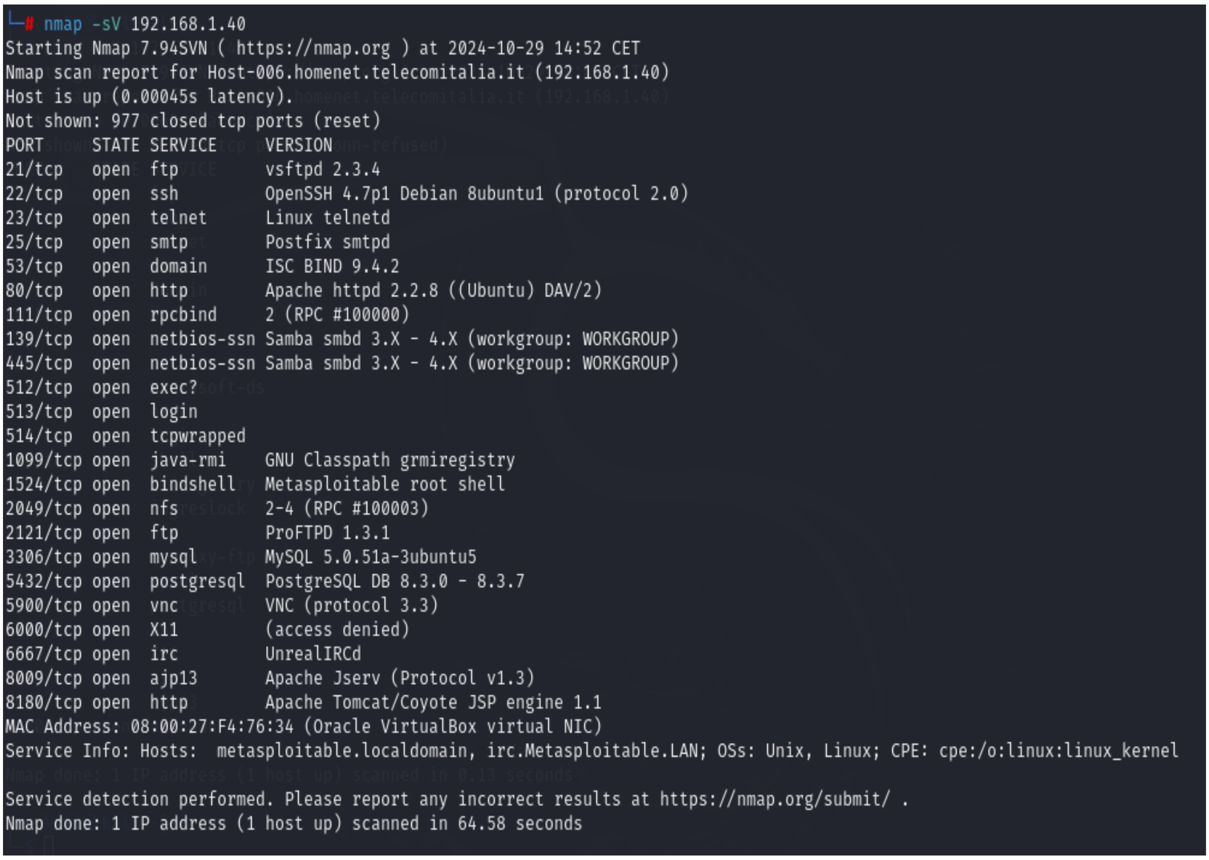
```
┌──(kali㉿kali)-[~]
└─$ nmap -sT 192.168.1.40
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 14:43 CET
Nmap scan report for Host-006.homenet.telecomitalia.it (192.168.1.40)
Host is up (0.0063s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
```

Version Detection:

Digitiamo sul terminale di Kali Linux il comando

“nmap -sV 192.168.1.40”

Grazie a questo comando possiamo vedere le versioni dei servizi utilizzati in esecuzione sulle porte aperte.



```
└─# nmap -sV 192.168.1.40
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 14:52 CET
Nmap scan report for Host-006.homenet.telecomitalia.it (192.168.1.40)
Host is up (0.00045s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec?
513/tcp  open  login
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:F4:76:34 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 64.58 seconds
```

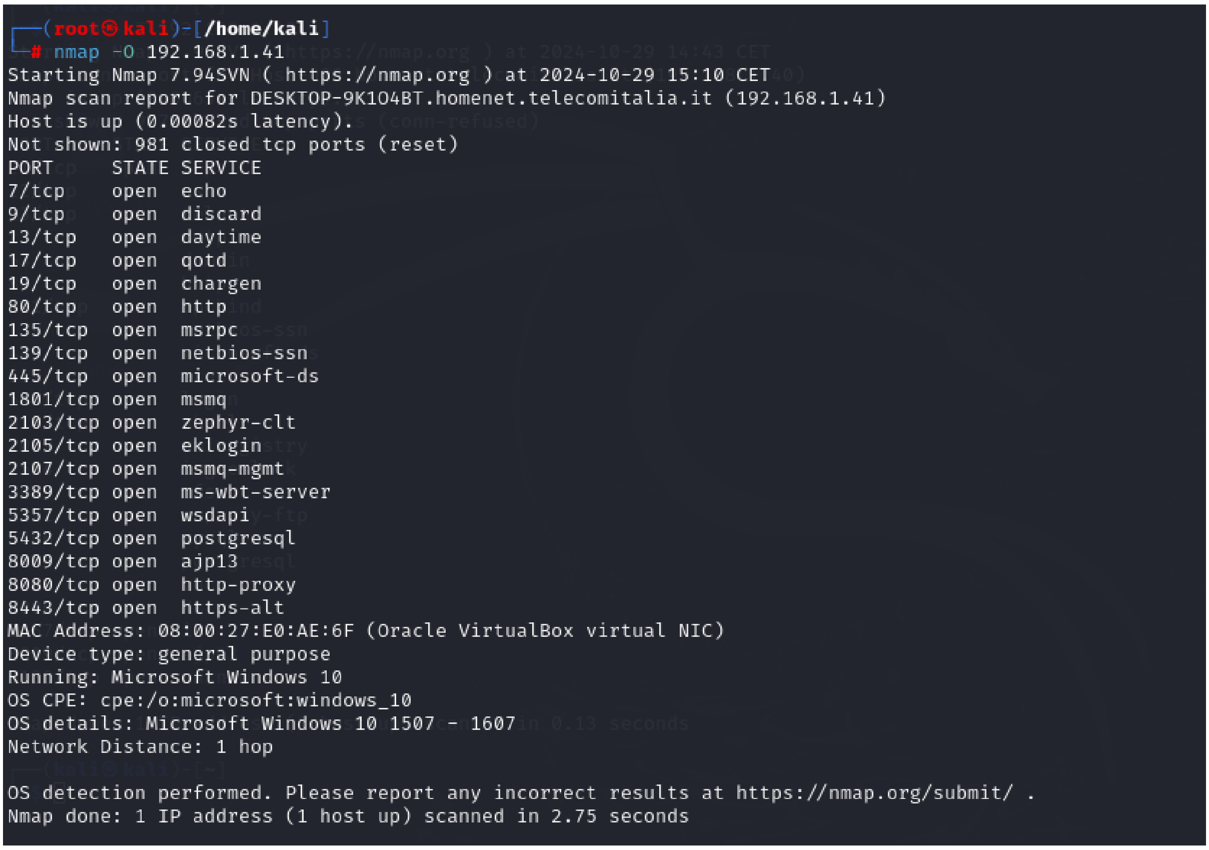
OS Fingerprint su Windows:

IP windows: 192.168.1.41

Digitiamo sul terminale di Kali Linux il comando

“nmap -O 192.168.1.41”

come fatto prima con Metasploitable ma eseguito su un indirizzo IP di un dispositivo Windows.



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.1.41
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 15:10 CET
Nmap scan report for DESKTOP-9K104BT.homenet.telecomitalia.it (192.168.1.41)
Host is up (0.00082s latency).
Not shown: 981 closed tcp ports (reset)
PORT     STATE SERVICE
7/tcp    open  echo
9/tcp    open  discard
13/tcp   open  daytime
17/tcp   open  qotd
19/tcp   open  chargen
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1801/tcp open  msmq
2103/tcp open  zephyr-clt
2105/tcp open  eklogin
2107/tcp open  msmq-mgmt
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi
5432/tcp open  postgresql
8009/tcp open  ajp13
8080/tcp open  http-proxy
8443/tcp open  https-alt
MAC Address: 08:00:27:E0:AE:6F (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1507 - 1607
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.75 seconds
```